



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,605	08/25/2006	Young-Man Park	B-5851PCT 623146-3	6256
36716	7590	06/21/2011	EXAMINER	
LADAS & PARRY 5670 WILSHIRE BOULEVARD, SUITE 2100 LOS ANGELES, CA 90036-5679			ABYANEH, ALI S	
		ART UNIT	PAPER NUMBER	
		2437		
		MAIL DATE	DELIVERY MODE	
		06/21/2011	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/562,605	PARK ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	ALI ABYANEH	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 08 April 2011.

2a) This action is **FINAL**.                            2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-21 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>01-27-2011</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application
	6) <input type="checkbox"/> Other: _____

### **DETAILED ACTION**

1. Claims 1-21 are presented for examination.
2. Claims 1, 3, 6, 8, 12, 15, 18 and 20 are amended.
3. In light of Applicant's amendment, the objection of claims 1, 3, 6-8, 12, 18 and 20 are withdrawn.
4. In light of Applicant's amendment, the previous rejection of claims 1-7, 18 and 19 under *35 USC § 112* (second paragraph) are withdrawn.

### **Response to Arguments**

5. Applicant's amendments/arguments filed on 04-18-2011 have been fully considered but are moot in view of the new ground(s) of rejection.

### **Examiner note**

6. Amended claims 1 and 18 do not include the text of the immediate prior version. For example prior version of claim 1, in step d, includes, "**according to an authentication success on the transmitted authenticator of the subscriber by the authentication server**". However, newly amended claim does not include such limitation. Amended claims must be presented with markings to indicate the changes that have been made relative to the immediate prior version. The changes in any amended claim must be shown by strike-through (for deleted matter) or underlining (for added matter). In order to expedite the procession a notice of non-compliance has not been issued and examiner has considered the limitation of "according to an

authentication success on the transmitted authenticator of the subscriber by the authentication server" as a deleted matter which applicant has inadvertently removed instated of showing the deletion by strike-through for the deleted matter.

Claim 18 includes similar error.

#### **Information Disclosure Statement PTO-1449**

7. The Information Disclosure Statement submitted by applicant on 01-27-2011 has been considered. Please see attached PTO-1449.

#### ***Claim Rejections - 35 USC § 112***

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 8 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 in step (e), line 21, recites: wherein the authenticator of the authentication server is authenticated by the subscriber station using a value which the subscriber station encrypts and generates as the encrypted value. It is not clear if "the encrypted value" is referring back to encrypted value of the step c ("the authentication server receiving an encrypted value") or "the encrypted value" is referring to the "value which subscriber station encrypts" in line 21 of the claim. For purpose of

the examination examiner considers “the encrypted value” is referring to the “value which subscriber station encrypts” in line 21 of the claim.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US Patent No. 6,996,714) in view of Mackenzie (US Publication No. 2002/0194478) further in view of Chen et al. (US Patent No. 5,784,463).

As per claim 1 and 18,

Halasz teaches in a key exchange method for mutual authentication at a subscriber station accessed to an authentication server through a wired/wireless communication, a two-factor authenticated key exchange method comprising: the subscriber station receiving a random number generated by the authentication server; encrypting a first predetermined value using the received random number, a password predefined in the subscriber station, and a key stored in a token, and transmitting the encrypted first predetermined value and a generated authenticator of the subscriber to the authentication server (column 7, lines 7-50);

the subscriber station receiving the authentication server's authenticator from the authentication server (column 7, lines 57-column 8, line 15).

Halasz does not explicitly teach the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server; authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. However, in an analogous art, Mackenzie teaches the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server (paragraph [0060], [0062]). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz to include the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to improve computational efficiency associated with network authentication and key exchange (paragraph

[0002]). Halasz in view of Mackenzie does not explicitly teach ; authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. However, in an analogous art, Chen teaches authenticating the generated authenticator of the subscriber using the encrypted first predetermined value (column 5, lines 48-54) and generates the authentication server's authenticator when the authentication is successful (column 5, lines 54-60); and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value (column 5, lines 58-62).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz and Mackenzie to include authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first

predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to secure a computer system from unauthorized access over an open or public network to which the computer is connected (column 1, lines 9-11).

As per claim 8 and 20,

Halasz teaches in a method for an authentication server accessed to a subscriber station for wired/wireless communication to exchange a key for mutual authentication, a two-factor authenticated key exchange method comprising: the authentication server receiving a key ; the authentication server using the value received from the subscriber station detecting the subscriber's password, the key stored in a token, and a public key of the authentication server, generating a random number, and transmitting the random number to the subscriber station; the authentication server receiving an encrypted value generated by the subscriber station and the subscriber's authenticator based on the transmitted random number (column 7, lines 7-50); the authentication server establishing a first predetermined value generated by using the password, the key stored in the token, and the random number to be a secret key, decrypting the encrypted value received to generate a second predetermined value, authenticating the

received authenticator of the subscriber based on the second predetermined value, and receiving the subscriber's authenticator when the authentication is successful; and the authentication server using the password, the key stored in the token, and, the public key, and transmitting the authenticator of the authentication server to the subscriber station (column 7, lines 57-column 8, line 15).

Halasz does not explicitly teach a key which is generated by the subscriber station by using an identifier and a public key of the authentication server, and wherein the authenticator of the authentication server is authenticated by the subscriber station using a value which the subscriber station encrypts and generates as the encrypted value. However, in an analogous art, Mackenzie teaches a key which is generated by the subscriber station by using an identifier and a public key of the authentication server (paragraph [0060]. [0062]).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz to include a key which is generated by the subscriber station by using an identifier and a public key of the authentication server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to improve computational efficiency associated with network authentication and key exchange (paragraph [0002]).

Halasz in view of Mackenzie does not explicitly teach wherein the authenticator of the authentication server is authenticated by the subscriber station using a value which the subscriber station encrypts and generates as the encrypted value. However, in an analogous art, Chane teaches the authenticator of the authentication server is authenticated by the subscriber station using a value which the subscriber station encrypts and generates as the encrypted value (column 5, lines 58-68).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz and Mackenzie to include the authenticator of the authentication server is authenticated by the subscriber station using a value which the subscriber station encrypts and generates as the encrypted value. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to secure a computer system from unauthorized access over an open or public network to which the computer is connected (column 1, lines 9-11).

As per claim 15,

Halasz teaches in a mutual authentication method through a two-factor authenticated key exchange between a subscriber station and an authentication server in a wireless communication system in which the subscriber station and the authentication server are accessed through an access point, an authentication method through a two-factor authenticated key exchange

comprising: the subscriber station receiving an identifier request from the access point (column 7, lines 39-42); the subscriber station transmitting a key ; the authentication server using the key received from the subscriber station, detecting the subscriber's password, the secret key, and the public key of the authentication server, generating a random number, and transmitting the random number to the subscriber station through the access point (column 7, lines 1-50); the subscriber station using the received random number, the password, and the key stored in the token, and transmitting an encrypted first predetermined value and the generated authenticator of the subscriber to the authentication server through the access point; the authentication server establishing a second predetermined value generated by using the password, the key stored in the token, and the random number to be a secret key, decrypting the encrypted value received , authenticating the received authenticator of the subscriber based on the decrypted value, and when the authentication is found successful, transmitting an authenticator of the authentication server generated by using the password, the key stored in the token, and the public key to the subscriber station through the access point; the subscriber station using the key stored in the token and the password, authenticating the received authenticator of the authentication server, and transmitting an authentication result to the authentication server through the access point; and the authentication server transmitting an access permission for the subscriber to the subscriber station through the access point when the authentication result transmitted from the

subscriber station is found successful (column 7, lines 45-column 8, line 15).

Halasz does not explicitly teach a key which is generated by using an identifier of the subscriber station and a public key of the authentication server to the authentication server through the access point; and wherein the authentication server's authentication is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station. However, in an analogous art, Mackenzie teaches a key which is generated by using an identifier of the subscriber station and a public key of the authentication server to the authentication server through the access point (paragraph [0060], [0062]).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz to include a key which is generated by using an identifier of the subscriber station and a public key of the authentication server to the authentication server through the access point. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to improve computational efficiency associated with network authentication and key exchange (paragraph [0002]).

Halasz in view of Mackenzie does not explicitly teach the authentication server's authentication is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station. However, in an analogous art, Chane teaches the authentication server's

authentication is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station (column 5, lines 58-68).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz and Mackenzie to include the authentication server's authentication is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to secure a computer system from unauthorized access over an open or public network to which the computer is connected (column 1, lines 9-11).

As per claim 2, 3, 9, 10, 16, 19 and 21,

Halasz furthermore teaches wherein the key stored in the token is a symmetric key; and before (a), the subscriber station determining the symmetric key and the password used for a symmetric key algorithm and sharing the symmetric key and the password with the authentication server during a registration process; and the subscriber station generating a random number and precomputing the first determined value when the subscriber station does not exchange a key for authentication with the authentication server (column 7, lines 35-column 8, line 15) .

As per claim 4 and 5,

Halasz furthermore teaches wherein the subscriber station stores the password and the public key of the authentication server in the token ( column 4, lines 30-39); wherein the generated key is generated by applying a one-way Hash function to an identifier of the subscriber station and the public key of the authentication server in (a) (column 5, lines 1-25).

As per claim 6,

Halasz furthermore teaches wherein (c) comprises: applying the Hash function to the received random number, the password, and the key stored in the token, and generating a second predetermined value; using the second predetermined value and encrypting the first predetermined value; using the random number and the first predetermined value, and generating the subscriber's session key; applying the Hash function to the generated session key, the password, the key stored in the token, and the identifier of the subscriber station, and generating the subscriber's authenticator; and transmitting the encrypted first predetermined value and the subscriber's authenticator to the authentication server (column 4, line 64, column 5, line 25).

As per claim 7,

Halasz furthermore teaches wherein (e) comprises: applying the Hash function to the subscriber's session key, the password, the key stored in the

token, and the public key of the authentication server, and generating a third predetermined value; determining whether the generated third predetermined value corresponds to the authenticator of the authentication server received from the authentication server; and determining that the authentication between the subscriber station and the authentication server is successful and receiving the authenticator of the authentication server when the generated third predetermined value is found to correspond to the authenticator of the authentication server (column 13, lines 12-27).

As per claim 11,

Halasz furthermore teaches wherein the authentication server stores the key stored in the token, the password, and the secret key of the authentication server in a security file database (column 5, lines 1-25).

As per claim 12,

Halasz furthermore teaches wherein (d) comprises: applying the Hash function to the password, the key stored in the token, and the random number, and generating the first predetermined value; establishing the generated first predetermined value to be a secret key, decrypting the received encrypted value, and generating the second predetermined value; using the generated second predetermined value, the public key of the authentication server, and the random number, and generating a session key of the authentication server; determining

whether the value obtained by applying the Hash function to the generated session key, the password, the key stored in the token, and an identifier of the subscriber station corresponds to the received authenticator of the subscriber; and determining that the authentication for the subscriber is found to be successful and receiving the authenticator of the subscriber when the value corresponds to the received authenticator of the subscriber (column 4, line 64, column 5, line 25).

As per claim 13,

Halasz furthermore teaches wherein the session key of the authentication server is used to generate the authenticator of the authentication server in (e) (column 4, lines 30-39).

As per claim 14,

Halasz furthermore teaches wherein the subscriber station transmits a user name, a hashed value of the public key of the authentication server, and a domain name to the authentication server when the identifier of the subscriber station uses the NAI (network access ID) format in order to support global roaming and billing in (a) (column 13, lines 12-27).

As per claim 17,

Halasz furthermore teaches wherein an extensible authentication protocol is used between the subscriber station and the access point, and a RADIUS protocol is used between the access point and the authentication server (column 3, lines 19-28).

### ***Conclusion***

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-

7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on **(571) 272-3867**. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/A. A./

Examiner, Art Unit 2437

/Eleni A Shiferaw/

Supervisory Patent Examiner, Art Unit 2437